DEPARTMENT OF THE ARMY
SAVANNAH DISTRICT, CORPS OF ENGINEERS
CESAS-IM P.O. BOX 889
SAVANNAH, GA 31402-0889

DISTRICT REGULATION
NO. 25-1-31

11 JUL 2005

Information Management
TELECOMMUNICATIONS MONITORING

1. Purpose. This regulation establishes monitoring requirements and procedures of Department of Defense (DOD) computers and other telecommunication systems used by Savannah District employees. All such systems are provided for the transmission of official Government communications and are subject to monitoring.

2. Applicability. This regulation covers appropriate actions to follow when a request is made to monitor these systems; i.e., email, telephone, cell phone, and internet.

3. Reference. Army Regulation 25-2, Information Assurance, 14 Nov 03.

4. Background. All telecommunications systems are provided for official government communications. These systems are subject to information systems security monitoring.

5. Responsibilities.

a. Commander. The Commander is appointed as the Delegated Approving Authority (DAA) for Savannah District. The DAA has the responsibility to ensure the district's network is secure as set forth and within guidelines, regulations and/or policies.

b. Information Assurance Manager. The Information Assurance Manager (IAM) has the responsibility to report any security violations and incidents to appropriate personnel; i.e., Commander.

c. Chief, Information Integration and Implementation Branch (IM-I) of Information Management Office. The Chief of IM-I has the responsibility to ensure appropriate information assurance (IA) tools are available and utilized, assign appropriate personnel to conduct monitoring, and ensure appropriate reports are produced in clear, interpretable format for submission to IAM.

d. Chief, Security and Law Enforcement (SL). The Chief of SL has the responsibility to ensure actions are taken promptly and notifying proper authorities; i.e., Department of Army, Criminal Investigation Command (CIC), Federal Bureaus of Investigations (FBI) or other investigative departments, if necessary and depending on nature of the monitoring results.

e. Office of Counsel. The IAM will confer with Office of Counsel for legal counsel to ensure code of ethics have been adhered to and actions are in compliance with any Department of Army and District regulations, policies and/or guidelines.

f. Users. Users of said systems shall have no expectation of privacy in any action; i.e., electronic documents stored, sent or received information on DOD computers and the use of other telecommunications systems; i.e., email, telephones and internet use.

6. Procedures. There are two types of monitoring categories, Category A and Category B. Category A is monitoring of the internet, telephones, and cell phones. Category B is monitoring of email.

a. Category A - Internet, Telephones and Cell Phones.

(1) Supervisors who believe their employees are abusing time spent on the internet, telephones, and cell phones should first attempt to resolve the issue with their employee (s).

(2) If it is deemed necessary for Information Management to collect data, the Division Chief shall submit a request, via email, to the IAM. The requests must include the type of monitoring to be performed, detailed justification as to why abuse is suspected and employee's name.

(3) If the IAM approves the request, the IAM will coordinate with the Chief of IM-I for data collection. Any data collected, per guidance by IAM, will be filed accordingly and marked as For Official Use Only (FOUO). Data collection is log information such as times and phone numbers of phone calls. Data collection does not include the recording of conversations.

(4) The IAM will submit findings to Division Chief for appropriate action.

b. Category B - Email.

(1) Supervisors who believe their employees are abusing the email system should first attempt to resolve the issue with their employees. Examples of email abuse include, but not limited to, unofficial advertising, selling or soliciting.

(2) If it is deemed necessary for Information Management to collect data, the Division Chief shall submit a request, via email, to the IAM. The requests must include the type of monitoring to be performed, detailed justification as to why abuse is suspected and employee's name.

(3) After initial request to collect data by Division Chief to IAM, IAM will confer with Office of Counsel (OC) for concurrence.

(4) Once OC concurrence is obtained, IAM and OC will present monitoring request to either Commander (DE) or Deputy Commander (DC) for approval.

(5) If DE or DC approval has been granted, IAM will coordinate with Chief, IM-I for action.

(6) Information collected will be provided to IAM and filed accordingly.

(7) The IAM will submit findings to Division Chief to determine appropriate action.

7. Exceptions. The sole exception to this policy is when information obtained during the monitoring requires immediate attention. Actions which interferes with the performance and integrity of network operations; is criminal in nature; i.e., child pornography, hate, and hacking; creates homeland security risks; puts individual(s) and/or organization in harm's way; i.e., death threats, bomb threats, etc.; and/or disclosure of classified information shall be brought to the immediate attention of the IAM. At such findings, the IAM notifies the Chief of SL and the Commander.

Mark S Held

MARK S. HELD
COL, EN
Commanding

DISTRIBUTION F